*e*Trust™ Agent for Cisco Network Admission Control (NAC)

Installation Guide

r1

G01028-1E

Computer Associates®

Contents

Chapter 1: Overview

This chapter provides a brief description of how the eTrust Agent for Cisco Network Admission Control (NAC) works and lists the Computer Associates applications that are currently NAC-enabled. In addition, this chapter describes system requirements and product components.

Note: This document assumes that Cisco NAC is fully installed and running in your network environment. For information about Cisco NAC, refer to the following Cisco documents:

Network Admission Control (NAC) home page:

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_sub_solution_home.html

NAC User Guide for Cisco Secure ACS 3.3

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080233612.html

NAC Attribute Management

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080233621.html#wp617627

How the eTrust Agent for Cisco NAC Works

The eTrust Agent for Cisco NAC discovers the posture attributes for Computer Associates applications on an end-point device that attempts to access or use resources on a network administered with Cisco NAC. The Cisco Trust Agent (CTA), also located on the end-point device, passes the posture attributes to a Cisco Access Control Server (ACS). The ACS compares the posture attributes with a set of policies previously defined by a network administrator. Based on the results of the comparison, the end-point device may either be granted full primary network access or placed into a separate virtual network, where the device can go through a remediation process before it is allowed to connect to the primary network.

Computer Associates NAC-Enabled Applications

The following Computer Associates applications are NAC-enabled:

- InoculateIT 6
- eTrust Antivirus r6, r7, r7.x
- eTrust PestPatrol Anti-Spyware r5
- eTrust PestPatrol Anti-Spyware Corporate Edition r5

The eTrust Agent for Cisco NAC discovers the posture attributes of these applications if they exist on an end-point device.

System Requirements

An end-point device running the eTrust Agent for Cisco NAC requires the following:

System Components
Pentium-class processor
Network connection

Operating System
English version of:
Windows NT, with Service Pack 6
Windows 2000
Windows XP Professional

Hard Disk Space
20 MB

Memory
128 MB for Windows NT and Windows 2000
256 MB for Windows XP

Software
Cisco Trust Agent 1.0

Product Components

The eTrust Agent for Cisco NAC consists of the following components:

cai-pp.txt
The cai-pp.txt file contains information for Computer Associates applications in the form of attribute/value pairs. You use this file with the CSUtil.exe program to add the Compute Associates product attribute definitions to the Cisco Secure ACS NAC database.

cai-pp.dll
The cai-pp.dll file is the eTrust Agent for NAC, which discovers the posture attributes of Computer Associates applications running on an end-point device. You use the CAPPInstall.exe program to install the plug-in on an end-point device.

cai-pp.inf
The cai-pp.inf file contains the eTrust Agent attribute definitions. The Cisco Trust Agent uses this file to communicate Computer Associates product attributes to the Cisco Secure ACS database.

Chapter 2: Setting Up eTrust Agent for Cisco NAC

This chapter contains procedures for setting up eTrust Agent for Cisco NAC. The set up process includes:

- Adding Computer Associates attributes to the Cisco Secure ACS NAC database
- Installing the Cisco Trust Agent on all end-point devices
- Installing the eTrust Agent for Cisco NAC on all end-point devices
- Verifying the installation

Note: The procedures in this chapter assume Cisco NAC is currently running in your network environment and is administered with Cisco Secure ACS 3.3.

Add Computer Associates Attributes to the NAC Database

Before you can define policies for Computer Associates posture attributes, you must first add the attribute/value pairs to the Cisco Secure ACS NAC database.

Note: The following procedure assumes Cisco Secure ACS 3.3 is installed at: C:\Program Files\CiscoSecure ACS v3.3

To add Computer Associates attributes to the Cisco Secure ACS NAC database, follow these steps:

1. Go to the Computer Associates SupportConnect website, http://supportconnect.ca.com, and locate the eTrust Agent for Cisco NAC.
2. Download the eTrust Agent for Cisco NAC to a system typically used for network management tasks.
3. Extract the contents of the downloaded zip file to a temporary directory, such as C:\Temp.
4. On the Cisco Secure ACS 3.3 for Windows system, copy the file cai-pp.txt to: C:\Program Files\CiscoSecure ACS v3.3\Utils

   The cai-pp.txt file contains the attribute/value pairs for NAC-enabled Computer Associates applications.
5. From the C:\Program Files\CiscoSecure ACS v3.3\Utils directory, run the following command:

   ```
   CSUtil.exe -addavp cai-pp.txt
   ```

   The CSUtil.exe program adds the attribute/value pairs to the Cisco Secure ACS NAC database.

Use the Cisco Secure ACS user interface to configure policies for Computer Associates products. For instructions, refer to the Cisco document *NAC User Guide for Cisco Secure ACS 3.3*.

Install the Cisco Trust Agent

Install the Cisco Trust Agent on all end-point devices, such as desktop computers, workstations, laptops, and servers that connect to or use network resources. Download and install the Cisco Trust Agent 1.0 from the Cisco website, http://www.cisco.com.

Install the eTrust Agent for Cisco NAC

Install the eTrust Agent for Cisco NAC on all end-point devices, such as desktop computers, workstations, laptops, and servers that connect to or use network resources.

To install the eTrust Agent for Cisco NAC on an end-point device, follow these steps:

1. From the directory you downloaded the eTrust Agent for Cisco NAC, distribute CAPPInstall.exe to all end-point devices.
2. Run the following command to silently install the eTrust Agent for NAC on the end-point device:

   ```
   CAPPInstall.exe -silent
   ```

   The files cai-pp.dll and cai-pp.inf are installed in %CommonProgramFiles%\Cisco Systems\CiscoTrustAgent\Plugins\Install. The next time the Cisco Trust Agent runs, these files are automatically moved up one directory level to \Plugins.

Verify the Installation

Use Cisco Secure ACS to verify that the Computer Associates attributes have been installed. For instructions, refer to the Cisco document *NAC User Guide for Cisco Secure ACS 3.3*.

To verify the installation of the eTrust Agent for Cisco NAC on an individual end-point device, restart the device and check that the following files exist in %CommonProgramFiles%\Cisco Systems\Cisco TrustAgent\Plugins:

- cai-pp.dll
- cai-pp.inf

For further assistance, see the Computer Associates SupportConnect website at http://supportconnect.ca.com, where you may check the Knowledge Base for additional information or contact a Customer Support representative.

Appendix A: Computer Associates Attribute Information

This appendix contains the attribute information for Computer Associates applications that are NAC-enabled. For information on how to manage NAC attributes, refer to the Cisco document *NAC Attribute Management*.

Application Types

The Cisco Trust Agent uses a Cisco-defined application type to uniquely identify and report posture attributes of NAC-enabled products from a single vendor. The following types apply to Computer Associates products:

Application	Type
eTrust Antivirus	3
eTrust PestPatrol Anti-Spyware	6

eTrust Antivirus Attributes

Cisco has defined eight standard NAC attributes for anti-virus applications. The eTrust Agent for Cisco NAC supports the reporting of these eight anti-virus attributes to the Cisco Secure ACS NAC database as follows:

Software-Name
The product name: eTrust Antivirus

Software-ID
The product ID as defined by Computer Associates: 1

Version
The product version number, as displayed in the eTrust Antivirus Version Information dialog

Scan-Engine-Version
The version of the currently active Realtime scan engine, as displayed in the Details for area of the eTrust Antivirus Version Information dialog

DAT-Version
The signature version of the currently active Realtime scan engine, as displayed in the Engine Information area of the eTrust Antivirus Version Information dialog

DAT-Date
The date and time the currently active Realtime scan engine was last updated, as displayed in the Engine Information area of the eTrust Antivirus Version Information dialog

Note: The Last Update date/time provides a more accurate representation of the device's posture than the Build Date of the virus signatures.

Protection-Enabled
Current status of Realtime Monitor: 1 if enabled, 0 if disabled

Action
A hexadecimal string that represents how infected files are treated by the Realtime scanner:
00000000 – Report only
00000001 – Cure
00000002 – Rename
00000003 – Delete
00000004 – Move

eTrust PestPatrol Anti-Spyware Attributes

Cisco has defined eight standard NAC attributes for anti-spyware applications. The eTrust Agent for Cisco NAC supports the reporting of these eight anti-spyware attributes to the Cisco Secure ACS NAC database as follows:

Software-Name
The name of the product, either eTrust PestPatrol Corporate Edition or eTrust PestPatrol

Software-ID
The product ID as defined by Computer Associates: 2

Version
The product version number:
eTrust PestPatrol Anti-Spyware: Version number of the file PestPatrol5.exe
eTrust PestPatrol Anti-Spyware Corporate Edition: The ImagePath value from "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PestPatrol Remote", and ProductVersion from version information resource of ppRemoteService.exe

Scan-Engine-Version
The version number of the eTrust PestPatrol COM control ppctl.dll

DAT-Version
Currently 5.0.0.x, where x is the current sequence number of pploc.dat as indicated in lfinfo.dat

DAT-Date
The creation date and time extracted from the database header of pploc.dat

Protection-Enabled
Current status of Active Protection: 1 if enabled, 0 if disabled

Action
Currently an empty string